Title: **Senior Information Security Engineer**
Department: Information Technology
Reports to: Associate Director, IT Security & Compliance

FLSA Status: Exempt
Internal Job Grade: 17

Position Summary

The Senior Information Security Engineer is responsible for assisting Access Health CT (AHCT) with its Risk Management Program, satisfying both regulatory compliance requirements and managing risk to an acceptable level. This is a hands-on role that is responsible for actively monitoring, maintaining, analyzing, implementing, triaging, advising, troubleshooting, and responding to ongoing security needs under the guidance of the Associate Director, IT Security & Compliance.

The Senior Information Security Engineer serves as a technical security subject-matter-expert and systems integrator for complex systems and/or networks, with a focus on securing vulnerabilities and reducing risk of system and/or asset compromises. Furthermore, this role will also assist with the continuous assessment of adequacy and effectiveness of IT security controls, provide expertise, development, and support to the risk mitigation plans across the organization collaborating with various functional areas and stakeholders, inclusive of vendors and partners. This role reports to the Associate Director of IT Security and Compliance and has no direct reports.

Responsibilities

- Lead and coordinate technical vulnerability assessments and security reviews of infrastructure, network, applications, and databases, utilizing Nessus scanning software and other state of the art security tools
- Facilitate, track, and manage vulnerability remediation based on risk categorization, communicating risk, and reporting on mitigation status
- Ensure compliance with results from vulnerability scans and/or penetration test outcomes
- Configure and use of the Security Information & Event Management (SIEM) platform, ensuring SIEM is fully utilized to monitor security events proactively inclusive of system logs and other monitoring data, and is in accordance with regulatory compliance requirements
- Monitor, analyze, and generate reports on company's security landscape utilizing SIEM and other state of the art security tools
- Design, configure, implement, maintain, and operate information system security controls and countermeasures
- Respond to information system security incidents, including investigation of, countermeasures to, and recovery from computer-based attacks, unauthorized access, and policy breaches; interact and coordinate with third-party incident responders, including law enforcement.
- Prepare incident response reports that take note of security incidents and action taken to mitigate risk
- Administer and audit authentication and access controls, including provisioning, changes, and deprovisioning of user and system accounts, security/access roles, and access permissions to information assets
- Provide security application knowledge and design concepts to Information Technology and Development teams

- Provide security expertise to support vendor and project security reviews and initiatives.
- Prepare and work with the different stakeholders to implement business continuity, system-wide disaster recovery and incident response plans
- Bridge information security requirements with business processes and IT systems and projects.
- Analyze trends, news and changes in threat and compliance environment with respect to organizational risk
- Develop and execute plans for compliance and mitigation of risk; perform risk and compliance self-assessments, and engage in and coordinate third-party risk and compliance assessments
- Develop and conduct tests for simulated cyber-attacks to identify any vulnerabilities in the network and application, and proactively take action to avoid an outside cyber-attack
- Analyze and recommend security controls and procedures in business processes related to use of information systems and assets, and monitor for compliance
- Analyze and develop information security governance, including organizational policies, procedures, standards, baselines and guidelines with respect to information security and use and operation of information systems
- Develop, administer, and provide advice, evaluation, and oversight for information security training and awareness programs
- Make recommendations and provide expertise to leadership regarding security advancements and current trends to best protect the company's systems and data
- Other duties as required

Qualifications

- Bachelor's degree in Management Information Systems, Cybersecurity, Computer Science or related IT field and/or equivalent industry experience
- A minimum of 5-7 years of combined hands-on experience in Information Security or Information Technology field
- One or more of the following security certifications is preferred or in process:
  - Certified Information Systems Security Professional (CISSP)
  - Certified in Risk and Information Systems Control (CRISC)
  - CompTIA Security+
  - Global Information Assurance Certification (GIAC)
- Strong knowledge of common Cybersecurity Frameworks including the National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF), NIST 800-53, Open Web Application Security Project (OWASP), and Center for Internet Security (CIS)
- Substantial and advanced experience with SIEM and vulnerability management lifecycle and tools such as Nessus, Burp Suite, Cisco AMP and Cisco Umbrella
- Experience with firewalls, IDS/IPS, endpoint solutions, proxy servers, data loss prevention, active directory, Java technology stack, cloud platforms, open source solutions, and exchange management/Office 365
- Experience with incident handling techniques and processes
- A solid understanding of cybersecurity best practices and how to implement them at a business-wide level
- Excellent problem-solving, analytical, and written/oral communication skills
- Ability to collaborate with internal and external stakeholders in an effective manner that produces desired results

- Ability to effectively meet business objectives in a highly collaborative and high-performance work environment
- Ability to manage and prioritize projects

Physical Demands: the physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

While performing the duties of this job, the employee is frequently required to sit, stand, hear, use hands to type data, and utilize a phone or other electronic communication devices. This employee may occasionally have to operate business machines. Specific vision abilities required in this job include close vision and the ability to adjust focus.

Work Environment: this is an in-office role 2 predetermined days per week and a remote role 3 days per week. The noise level in the work environment is usually moderate. The role requires the ability to work offsite with stakeholders at their locations, e.g., BITS, DSS. Requires fast-paced deadlines and has a high stress at times. Frequent local travel and some travel within the U.S.

Affirmative Action and Equal Opportunity Employer